Prepared Testimony and Statement for the Record of

Marc Rotenberg,
President, EPIC

Hearing on

"Protecting Consumer's Data: Policy Issues Raised by Choicepoint"

Before the

Subcommittee on Commerce, Trade and Consumer Protection,
Committee on Energy and Commerce,
U.S. House of Representatives

March 15, 2005
2123 Rayburn House Office Building
Washington, DC

Mr. Chairman, and members of the Committee, thank you for the opportunity to appear before you today. My name is Marc Rotenberg and I am Executive Director and President of the Electronic Privacy Information Center in Washington, DC. EPIC is a non-partisan public interest research organization established in 1994 to focus public attention on emerging civil liberties issues. We are very pleased that you have convened this hearing today on protecting consumer's data and the policy issues raised by Choicepoint.

In my statement today, I will summarize the significance of the Choicepoint matter, discuss EPIC's efforts to bring public attention to the problem before the incident was known, suggest several lessons that can be drawn from this matter, and then make several specific recommendations.[1]

The main point of my testimony today is to make clear the extraordinary urgency of addressing the unregulated sale of personal information in the United States and how the data broker industry is contributing to the growing risk of identity theft in the United States. Whatever your views may be on the best general approach to privacy protection, Choicepoint has made clear the need to regulate the information broker industry.

The Significance of the Choicepoint Matter

With all the news reporting of the last several weeks, it has often been difficult to tell exactly how a criminal ring engaged in identity theft obtained the records of at least 145,000 Americans. According to some reports, there was a computer "break-in. "Others described it as "theft."[2] In fact, Choicepoint simply sold the information.[3] This is Choicepoint's business and it is the business of other companies that are based primarily on the collection and sale of detailed information on American consumers. In this most recent case, the consequences of the sale were severe.

According to California police, at least 750 people have already suffered financial harm.[4] Investigators believe data on least 400,000 individuals may have been compromised.[5] Significantly, this was not an isolated incident. Although Choicepoint CEO Derek Smith said that the recent sale was the first of its kind, subsequent reports

[1] Many other organizations have also played a critical role in drawing attention to the growing problem of identity theft. These include Consumers Union, the Identity Theft Resource Center, Privacy International, the Privacy Rights Clearinghouse, the Privacy Times, the US Public Interest Research Group, and the World Privacy Forum.
[2] Associated Press, "ChoicePoint hacking attack may have affected 400,000," Feb. 17, 2005, *available at* http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/10920220.htm.
[3] Robert O'Harrow Jr., "ID Theft Scam Hits D.C. Area Residents," Washington Post, Feb. 21, 2005, at A01.
[4] Bob Sullivan, "Data theft affects 145,000 nationwide," MSNBC, Feb. 18, 2005, *available at* http://www.msnbc.msn.com/id/6979897/.
[5] Associated Press, "ChoicePoint hacking attack may have affected 400,000," Feb. 17, 2005, *available at* http://www.ledger-enquirer.com/mld/ledgerenquirer/news/local/10920220.htm.

revealed that Choicepoint also sold similar information on 7,000 people to identity thieves in 2002 with losses over $1 million.[6] And no doubt, there may have been many disclosures before the California notification law went into effect as well as more recent disclosures of which that we are not yet aware.

The consumer harm that results from the wrongful disclosure of personal information is very clear. According to the Federal Trade Commission, last year 10 million Americans were affected by identity theft. Identity theft is the number one crime in the country. For the fifth year in a row, identity theft topped the list of complaints, accounting for 39 percent of the 635,173 consumer fraud complaints filed with the agency last year.[7] And there is every indication that the level of this crime is increasing.

Choicepoint is not the only company that has improperly disclosed personal information on Americans. Bank of America misplaced back-up tapes containing detailed financial information on 1.2 million employees in the federal government, including many members of Congress.[8] Lexis-Nexis made available records from its Seisint division on 32,000 Americans to a criminal ring that exploited passwords of legitimate account holders.[9] DSW, a shoe company, announced that 103 of its 175 stores had customers' credit and debit card information improperly accessed.[10]

But there are factors that set Choicepoint apart and make clear the need for legislation for the information broker industry. First, Choicepoint is the largest information broker in the United Stares. The company has amassed more than 19 billion records and has acquired a large number of smaller companies that obtain everything from criminal history records and insurance claims to DNA databases. The private sector and increasingly government rely on the data provided by Choicepoint to determine whether Americans get home loans, are hired for jobs, obtain insurance, pass background checks, and qualify for government contracts.

Choicepoint has become the true invisible hand of the information economy. Its ability to determine the opportunities for American workers, consumers, and voters is without parallel.

Second, the Choicepoint databases are notoriously inaccurate. A recent article in MSNBC, "Choicepoint files found riddled with errors," recounts the extraordinary errors

---

[6] David Colker and Joseph Menn, "ChoicePoint CEO Had Denied Any Previous Breach of Database," Los Angeles Times, March 3, 2005, at A01.

[7] Federal Trade Commission, "FTC Releases Top 10 Consumer Complaint Categories for 2004," (Feb. 1, 2005), *available at* http://www.ftc.gov/opa/2005/02/top102005.htm.

[8] Robert Lemos, "Bank of America loses a million customer records," CNet News.com, Feb. 25, 2005, *available at* http://earthlink.com.com/Bank+of+America+loses+a+million+customer+records/2100-1029_3-5590989.html?tag=st.rc.targ_mb.

[9] Jonathan Krim and Robert O'Harrow, Jr., "LexisNexis Reports Theft of Personal Data," Washingtonpost.com, March 9, 2005, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A19982-2005Mar9?language=printer.

[10] Associated Press, "Credit Information Stolen From DSW Stores," March 9, 2005, *available at* http://abcnews.go.com/Business/wireStory?id=563932&CMP=OTC-RSSFeeds0312.

in just one Choicepoint report that was provided to a privacy expert. [11] Among the statements in the 20-page National Comprehensive Report was an inaccurate entry that described "possible Texas criminal history" and a recommendation for a follow-up search. The report listed an ex-boyfriend's address, even though she had never lived with the fellow. As MSNBC reporter Bob Sullivan writes, "The report also listed three automobiles she never owned and three companies listed that she never owned or worked for."

The report on the document provided to Deborah Pierce is very similar to an earlier report described by another privacy expert Richard Smith, "who paid a $20 fee and received a similar report from Choicepoint several years ago. The company offers a wide variety of reports on individuals; Smith purchased a commercial version that's sold to curious consumers. Smith's dossier had the same kind of errors that Pierce reported. His file also suggested a manual search of Texas court records was required, and listed him as connected to 30 businesses that he knew nothing about."

Third, Choicepoint and other information brokers have spent a great deal of time and money trying to block effective privacy legislation in Congress. According to disclosure forms filed with the U.S. House and Senate, obtained by the Wall Street Journal, Choicepoint and six of the country's other largest sellers of private consumer data spent at least $2.4 million last year to lobby members of Congress and a variety of federal agencies. The Journal reports that, "Choicepoint was the biggest spender, with $970,000 either paid to outside lobbyists or spent directly by the company."[12]

This improper disclosure and use of personal information is contributing to identity theft, which is today the number one crime in the United States. According to a 2003 survey by the Federal Trade Commission, over a one-year period nearly 5% of the adult populations were victims of some form of identity theft.[13]

EPIC's Efforts to Bring Public Attention to the Problems with Choicepoint

Well before the recent news of the Choicepoint debacle became public, EPIC had been pursuing the company and had written to the FTC to express deep concern about its business practices and its ability to flout the law. On December 16, 2004, EPIC urged the Federal Trade Commission to investigate Choicepoint and other data brokers for compliance with the Fair Credit Reporting Act (FCRA), the federal privacy law that helps

[11] Bob Sullivan, "ChoicePoint files found riddled with errors Data broker offers no easy way to fix mistakes, either, " MSNBC, March 8, 2005, *available at* http://www.msnbc.msn.com/id/7118767/.

[12] Evan Perez and Rick Brooks, "Data Providers Lobby to Block More Oversight," *Wall Street Journal*, March 4, 2005, at B1.

[13] Federal Trade Commission, "Identity Theft Survey Report" (Sept. 2003), available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

insure that personal financial information is not used improperly. [14] The EPIC letter said that Choicepoint and its clients had performed an end-run around the FCRA and was selling personal information to law enforcement agencies, private investigators, and businesses without adequate privacy protection.

Choicepoint wrote back to us to say, in effect, that there was no problem The company claimed to fully comply with FCRA and that the question of whether FCRA, or other federal privacy laws, should apply to all of its products as simply a policy judgment. It made this claim at the same time it was spending several million dollars over the last few years to block the further expansion of the FCRA.

Mr. Chairman, hindsight may be 20-20, but it is remarkable to us that Choicepoint had the audacity to write such a letter when it already knew that state investigators had uncovered the fact that the company had sold information on American consumer to an identity theft ring. They were accusing us of inaccuracy at the same time that state and federal prosecutors knew that Choicepoint, a company that offered services for business credentialing, had exposed more than a hundred thousand Americans to a heightened risk of identity theft because it sold data to crooks.

But the problems with Choicepoint long preceded this recent episode. Thanks to Freedom of Information Act requests relentlessly pursued by EPIC's Senior Counsel Chris Hoofnagle, we have obtained over the last several yeas extraordinary documentation of Choicepoint's growing ties to federal agencies and the increasing concerns about the accuracy and legality of these products.[15] So far, EPIC has obtained FOIA documents from nine different agencies concerning Choicepoint. Much of the material is available on our web site at http:www.epic.org/privacy/Choicepoint. One document from the Department of Justice, dated December 13, 2002, discusses a "Report of Investigation and Misconduct Allegations . . . Concerning Unauthorized Disclosure of Information." [16] There are documents from the IRS that describe how the agency would mirror huge amounts of personal information on IRS computers so that Choicepoint could perform investigations. [17] Several documents describe Choicepoint's sole source contracts with such agencies as the United States Marshals Service and the FBI. [18]

Among the most significant documents obtained by EPIC were those from the Department of State, which revealed the growing conflicts between the United States and foreign governments that resulted from the efforts of Choicepoint to buy data on citizens across Latin America for use by the US federal law enforcement agencies. [19] One document lists news articles that were collected by the agency to track outrage in Mexico

[14] Letter from Chris Jay Hoofnagle, Associate Director, EPIC, and Daniel J. Solove, Associate Professor, George Washington University Law School, to Federal Trade Commission, Dec. 16, 2004, *available at* http://www.epic.org/privacy/choicepoint/fcraltr12.16.04.html.
[15] EPIC v. Dep't of Justice et al., No. 1:02cv0063 (CKK)(D.D.C.).
[16] *Available at* http://www.epic.org/privacy/choicepoint/default.html.
[17] *Id*.
[18] *Id*.
[19] *Available at* http://www.epic.org/privacy/choicepoint/default.html.

and other countries over the sale of personal information by Choicepoint.[20] A second document contains a cable from the American Embassy in Mexico to several different government agencies warning that a "potential firestorm may be brewing as a result of the sale of personal information by Choicepoint.[21] A third set of documents describes public relations strategies for the American Embassy to counter public anger surrounding the release of personal information of Latin Americans to Choicepoint.[22]

Choicepoint's activities have fueled opposition to the United States overseas and raised the alarming prospect that our country condones the violation of privacy laws of other government.[23] As USA Today reported on September 1, 2003:

> After the Mexican government complained that its federal voter rolls were the source, and were likely obtained illegally by a Mexican company that sold them to Choicepoint, the suburban Atlanta company cut off access to that information.
>
> In June, ChoicePoint wiped its hard drives of Mexicans' home addresses, passport numbers and even unlisted phone numbers. The company also backed out of Costa Rica and Argentina.
>
> ChoicePoint had been collecting personal information on residents of 10 Latin American countries — apparently without their consent or knowledge — allowing three dozen U.S. agencies to use it to track and arrest suspects inside and outside the United States.[24]
>
> The revelations helped kindle privacy movements in at least six countries where the company operates. Government officials have ordered — or threatened — inquiries into the data sales, saying ChoicePoint and the U.S. government violated national sovereignty.

Lessons of Choicepoint

The Choicepoint incident proves many important lessons for the Congress as it considers how best to safeguard consumer privacy in the information age.

First, it should be clear now that privacy harms have real financial consequences. In considering privacy legislation in the past, Congress has often been reluctant to recognize the actual economic harm that consumers suffer when their personal information is misused, when inaccurate information leads to the loss of a loan, a job, or

---

[20] *Id*.
[21] *Id*.
[22] *Id*.
[23] EPIC and Privacy International, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* 123-24, 182, 493 (2004) (Public Records, Argentina country report, Mexico country report)
[24] Associated Press, "Vendor sells Latin American citizen data to U.S.," Sept. 1, 2003, *available at* http://www.usatoday.com/tech/news/techpolicy/2003-09-01-choicepoint_x.htm.

insurance. Consumers suffer harms both from information that is used for fraud and inaccurate information that leads to lost opportunities through no fault of the individual.

A clear example of how the company has contributed to the growing problem of identity theft may be found in Choicepoint's subscriber agreement for access to AutoTrackXP, a detailed dossier of individuals' personal information. A sample AutoTrackXP report on the ChoicePoint web site shows that it contains Social Security Numbers; driver license numbers; address history; phone numbers; property ownership and transfer records; vehicle, boat, and plane registrations; UCC filings; financial information such as bankruptcies, liens, and judgments; professional licenses; business affiliations; "other people who have used the same address of the subject," "possible licensed drivers at the subject's address," and information about the data subject's relatives and neighbors.[25] This sensitive information is available to a wide array of companies that do not need to articulate a specific need for personal information each time a report is purchased. Choicepoint's subscriber agreement shows that the company allows access to the following businesses: attorneys, law offices, investigations, banking, financial, retail, wholesale, insurance, human resources, security companies, process servers, news media, bail bonds, and if that isn't enough, Choicepoint also includes "other."

Second, it should be clear that market-based solutions fail utterly when there is no direct relationship between the consumer and the company that proposed to collect and sell information on the consumer. While we continue to believe that privacy legislation is also appropriate for routine business transactions, it should be obvious to even those that favor market-based solutions that this approach simply does not work where the consumer exercises no market control over the collection and use of their personal information. As computer security expert Bruce Schneier has noted, "ChoicePoint doesn't bear the costs of identity theft, so ChoicePoint doesn't take those costs into account when figuring out how much money to spend on data security."[26] This argues strongly for regulation of the information broker industry.

Third, there are clearly problems with both the adequacy of protection under current federal law and the fact that many information products escape any kind privacy rules. Choicepoint has done a remarkable job of creating detailed profiles on American consumers that they believe are not subject to federal law. Products such as AutoTrackXP are as detailed as credit reports and have as much impact on opportunities in the marketplace for consumers as credit reports, yet Choicepoint has argued that they should not be subject to FCRA. Even their recent proposal to withdraw the sale of this information is not reassuring. They have left a significant loophole that will allow them to sell the data if they believe there is a consumer benefit. [27]

---

[25] ChoicePoint, AutoTrackXP Report, http://www.choicepoint.com/sample_rpts/AutoTrackXP.pdf.

[26] "Schneier on Security: Choicepoint" *available at* http://www.schneier.com/blog/archives/2005/02/choicepoint.html.

[27] Aleksandra Todorova, "ChoicePoint to Restrict Sale of Personal Data," Smartmoney.com, March 4, 2005, *available at* http://www.smartmoney.com/bn/index.cfm?story=20050304015004.

But even where legal coverage exists, there is insufficient enforcement, consumers find it difficult to exercise their rights, and the auditing is non-existent. According to EPIC's research, there is no indication that commercial data brokers audit their users and refer wrongdoers for prosecution. In other words, in the case where a legitimate company obtains personal information, there is no publicly available evidence that Choicepoint has any interest in whether that information is subsequently used for illegitimate purposes.

Law enforcement, which has developed increasingly close ties to information brokers such as Choicepoint seems to fall entirely outside of any auditing procedures. This is particularly troubling since even those reports that recommend greater law enforcement use of private sector databases for public safety recognize the importance of auditing to prevent abuse.[28]

And of course there are ongoing concerns about the broad permissible purposes under the FCRA, the use of credit header information to build detailed profiles, and the difficulty that consumers continue to face in trying to obtain free credit reports that they are entitled to under the FACTA.

Fourth, we believe this episode also demonstrates the failure of the FTC to aggressively pursue privacy protection. We have repeatedly urged the FTC to look into these matters. While on some occasions, the FTC has acted. [29] But too often the Commission has ignored privacy problems that are impacting consumer privacy and producing a loss of trust and confidence in the electronic marketplace. In the late 1990s, the FTC promoted self-regulation for the information broker industry and allowed a weak set of principles promulgated as the Individual References Service Group to take the place of effective legislation. It may well be that the Choicepoint fiasco could have been avoided if the Commission chose a different path when it considered the practices of the information broker industry.

The FTC has also failed to pursue claims that it could under section 5 of the FTC Act that prohibits unfair practices. Practices are unfair if they cause or are likely to cause consumers substantial injury that is neither reasonably avoidable by consumer nor offset by countervailing benefits to consumers and competition.[30] It may be that the unfairness doctrine could be applied in cases where there is no direct relationship between the consumer and the company, but to date the FTC has failed to do this. [31]

---

[28] See Chris J. Hoofnagle, "Big Brother's Little Helpers: How Choicepoint and Other Commercial Data brokers Collect, process, and Package Your Data for Law Enforcement," *University of North Carolina Journal of International Law & Commercial Regulation* (Summer 2004), available at http://ssrn.com/abstract=582302.

[29] *See* FTC's investigation into Microsoft's Passport program. Documentation *available at* http://www.epic.org/privacy/consumer/microsoft/passport.html.

[30] 15 U.S.C. 45(n); Letter from Michael Pertschuk, FTC Chairman, and Paul Rand Dixon, FTC Commissioner, to Wendell H. Ford, Chairman, House Commerce Subcommittee on Commerce, Science, and Transportation (Dec. 17, 1980), at http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

[31] In *FTC v. Rapp*, the "Touch Tone" case, the FTC pursued private investigators engaged in "pretexting," a practice where an individual requests personal information about others under false pretenses. No. 99-WM-

Fifth, we believe the Choicepoint episode makes clear the importance of state-based approaches to privacy protection. Congress simply should not pass laws that tie the hands of state legislators and prevent the development of innovative solutions that respond to emerging privacy concerns. Many states are today seeking to establish strong notification procedures to ensure that their residents are entitled to at least the same level of protection as was provided by California.[32]

In this particular case, the California notification statute helped ensure that consumers would at least be notified that they are at risk of heightened identity theft. This idea makes so much sense that 38 attorney generals wrote to Choicepoint to say that their residents should also be notified if their personal information was wrongly disclosed. [33] Choicepoint could not object. It was an obvious solution.

Finally, there is still a lot we do not know about the Choicepoint company. This firm has expanded so rapidly and acquired so many companies in the last few years, it is very difficult to assess how much information it actually has on Americans. As a starting point for further work by the Committee, I would urge you and Committee Staff to obtain your own Choicepoint records in the AutoTrackXP service as well as the National Comprehensive Report. This is the information about you that Choicepoint sells to strangers. If you want to understand the serious problem of record accuracy, this is one good place to start.

Recommendations

Clearly, there is a need for Congress to act. Although Choicepoint has taken some steps to address public concerns, it continues to take the position that it is fee to sell personal information on American consumers to whomever it wishes where Choicepoint, and not the consumer, believes there "consumer-driven benefit or transaction."[34] Moreover, the company remains free to change its policies at some point in the future, and the steps taken to date do not address the larger concerns across the information broker industry.

---

783 (D. Colo. 2000), 2000 U.S. Dist. LEXIS 20627. In a typical scheme, the investigator will call a bank with another's Social Security Number, claim that he has forgotten his bank balances, and requests that the information be given over the phone. The FTC alleged that this practice of the defendants, was deceptive and unfair. It was deceptive because the defendants deceived the bank in providing the personal information of another. The practice was unfair in that it occurs without the knowledge or consent of the individual, and it is unreasonably difficult to avoid being victimized by the practice.

[32] "Choicepoint Incident Prompts State Lawmakers to Offer Data Notification Bills," 10 *BNA Electronic Commerce & Law Report* 217-18 (March 9, 2005)

[33] Associated Press, "38 AGs send open letter to ChoicePoint," *available at* http://www.usatoday.com/tech/news/computersecurity/infotheft/2005-02-19-ag-letter-to-choicepoint_x.htm.

[34] "Choicepoint Halts Sale of Sensitive Information, as Agencies Launch Probes," 10 *BNA Electronic Commerce and Law Report* 219 (March 9, 2005).

Modest proposals such as the extension of the Gramm-Leach-Bliley Act's Security Safeguards Rule are unlikely to prevent future Choicepoint debacles. The Safeguards Rule merely requires that financial institutions have reasonable policies and procedures to ensure the security and confidentiality of customer information. Recall that the disclosure by Choicepoint did not result from a "hack" or a "theft" but from a routine sale. Moreover, the Security Safeguards Rule will do nothing to give consumers greater control over the transfer of their personal information to third parties or to promote record accuracy.

Extending notification statutes such as the California bill would be a sensible step but this is only a partial answer. Notification only addresses the problem once the disclosure has occurred. The goal should be to minimize the likelihood of future disclosure. It is also important to ensure that any federal notification bill is as least as good as the California state bill and leaves the states the freedom to develop stronger and more effective measures. What happens for example, when at some point in the future, we must contend with the extraordinary privacy problems that will result from the disclosure of personal information contained in a database built on biometric identifiers?

At this time, legislation such as the Information Protection and Security Act, H.R. 1080, provides a good starting point to safeguard consumer privacy and reduce the growing threat of identity theft. It would allow the FTC to develop fair information practices for data brokers; violators would be subject to civil penalties. Enforcement authority would be given to the FTC and state attorneys general. Consumers would be able to pursue a private right of action, albeit a modest one. And states would be free to develop stronger measures if they chose.

But a stronger measure would establish by statute these same authorities and impose stricter reporting requirements on the information broker industry. It would include a liquidated damages provision that sets a floor, not a limit, on damages when a violation occurs, as is found in other privacy laws. It is even conceivable that Congress could mandate that information brokers provide to consumers the same information that they propose to sell to a third party prior to the sale. This would make consent meaningful. It would promote record accuracy. And it would allow the consumer to determine for himself or herself whether in fact the transaction will provide a "consumer-driven benefit." Proposals for credit report "freeze" legislation that allow consumers to determine when it is in their benefit to release personal credit information provides a good parallel for strong legislation in the data broker field.

Furthermore, to the extent that information brokers, such as Choicepoint, routinely sell data to law enforcement and other federal agencies, they should be subject to the federal Privacy Act. A "privatized intelligence service," as Washington Post reporter Robert O'Harrow has aptly described the company, Choicepoint should not be

permitted to flout the legal rules that help ensure accuracy, accountability, and due process in the use of personal information by federal agencies. [35]

Also, a very good framework has been put forward by Professor Daniel Solove and EPIC's Chris Hoofnagle. [36] This approach is similar to other frameworks that attempt to articulate Fair Information Practices in the collection and use of personal information. But Solove and Hoofnagle make a further point that is particularly important in the context of this hearing today on Choicepoint. Increasingly, the personal information made available through public records to enable oversight of government records has been transformed into a privatized commodity that does little to further government oversight but does much to undermine the freedom of Americans. While EPIC continues to favor strong open government laws, it is clearly the case that open government interests are not served when the government compels the production of personal information, sells the information to private data vendors, who then make detailed profiles available to strangers. This is a perversion of the purpose of public records.

Looking ahead, there is a very real risk that the consequences of improper data use and data disclosure are likely to accelerate in the years ahead. One has only to look at the sharp increase in identity theft documented by the Federal Trade Commission, consider the extraordinary rate of data aggregation in new digital environments, as well as the enormous efforts of the federal government to build ever more elaborate databases to realize that the risk to personal privacy is increasing rapidly. Congress can continue to deal with these challenges in piecemeal fashion, but it seems that the time has come to establish a formal government commission charged with the development of long-terms solutions to the threats associated with the loss of privacy. Such a commission should be established with the clear goal of making specific proposals. It should include a wide range of experts and advocates. And it should not merely be tasked with trying to develop privacy safeguards to counter many of the government new surveillance proposals. Instead, it should focus squarely on the problem of safeguard privacy.

Congress needs to establish a comprehensive framework to safeguard the right of privacy in the twenty-first century. With identity theft already the number one crime, and the recent spate of disclosures, any further delay could come at enormous cost to American consumers and the American economy.

Finally, Mr. Chairman, there are several practical questions left open by the Choicepoint matter. First, as we said to the FTC in December, Choicepoint has done a poor job tracking he use of personal information on American consumers that it routinely sells to strangers. Now is the time for Choicepoint to go back to its audit logs and determine what the legal basis was for selling the information that was provided to the identity theft ring. In fact, we believe that Choicepoint should be required to review all of

[35] Robert O'Harrow, *No Place to Hide: Behind the Scenes of Our Emerging Surveillance Society* (Free Press 2005).
[36] Daniel Solove and Chris Jay Hoofnagle, "A Model Regime of Privacy Protection," March 8, 2005, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=681902.

its audit logs for the past year and report to this committee on whether it has uncovered any other instance of breaches within the company. Just as heads of financial companies are now required to vouch for the accuracy of their financial statements, the heads of the information broker companies should be required to make an annual representation tot he public that they have reviewed the audit logs of their companies and are assured that the information they have disclosed has only been used for lawful purposes.

Second, there is the question of what Choicepoint intends to do with the money that it received from the sale of personal information to an identity theft ring. How can Choicepoint possibly keep the funds from those transactions? In a letter that EPIC sent to Choicepoint COO Douglas Curling, we urged the company to "disgorge the funds that you obtained from the sale of the data and make these funds available to the individuals who will suffer from identity theft as a result of this disclosure." Since Mr. Smith, the company's President is at the hearing today, perhaps he can explain what Choicepoint will do with the funds.

Third Choicepoint has still not provided to the victims of the negligent sale the same information that it disclosed to the identity thieves. At the very least, we think the company should give people the same records it sold to the crooks.

Conclusion

For many years, privacy laws came up either because of the efforts of a forward-looking Congress or the tragic experience of a few individuals. Now we are entering a new era. Privacy is no longer theoretical. It is no longer about the video records of a federal judge or the driver registry information of a young actress. Today privacy violations affect hundreds of thousands of American all across the country. The harm is real and the consequences are devastating.

Whatever one's view may be of the best general approach to privacy protection, there is no meaningful way that market-based solutions can protect the privacy of American consumers when consumers have no direct dealings with the companies that collect and sell their personal information. There is too much secrecy, too little accountability, and too much risk of far-reaching economic damage. The Choicepoint debacle has made this clear.

The Committee may not be able to solve every privacy problem, but I urge you today to focus on the information broker industry and to pass legislation such as the Information Protection and Security Act. The information broker industry has been flying under the radar for too long.

I appreciate the opportunity to be here today. I will be pleased to answer your questions

References

EPIC Choicepoint Page, available at http://www.epic.org/privacy/choicepoint/